Last Time: Fund. Thm. of Arith. ✱

"Every positive integer is a product of primes".

Remark: "Cyber Security" is a reason to care about number theory...

Claim: Factoring is hard (even for a computer)...

148 973 017 005 173

↳ 30 more digits...

↳ 300 more digits...

Point: Data encryption can be done leveraging this fact...

(Look up the "RSA encryption scheme").

Warning: Don't implement this for secure use yourself...

↝ Challenge: learn about RSA, and write a simple implementation...

Enumeration.

Recall: The cardinality of a set S is

$\#S = |S|$ = "the number of elements in S".

Defn: A set S is finite when $\#S \in \mathbb{N}_0$, and infinite otherwise.

Fundamental Question: ✱ Given a finite set, what is its cardinality? [Is there an expression for the cardinality which is meaningful to the set itself?]

Philosophical Question...

Ex: Let $n \in \mathbb{N}_0$. Then $\#[n] = n$.

NB: $[n] = \{1, 2, \cdots, n\}$.

Ex: Suppose you're given a bag w/ red, green, and blue marble And another bag w/ red, green, and blue dice. (1 of each color is in each bag). How many ways can you choose a pair of die and a marble?

Sol: Brute force:

		R	B	G
→	R	RR	RB	RG
	B	BR	BB	BG
	G	GR	GB	GG

↑ Colors of Die

Colors of marble ↗

→ 9 possibilities.

Ex: Suppose Bag 1 has 1 marble each of 5743 colors, and Bag 2 has 1 die each of 7292 colors. How many marble-die pairs are there?

IDEA: First we choose a marble. ← 5743 options
Then we choose a die. ← 7292 options

Point: For every marble choice we have the same number of choices of a die...

we should therefore obtain a chart (like above) w/ 5743 columns and 7292 rows to count the options. So we expect 5743×7292 possible marble-die pairs...

NB: The "chart" is a fancy way of expressing the cartesian product of the sets of options (in an example like this).

Prop: Given sets A, B. The cardinality of the product satisfies $\#(A \times B) = (\#A)(\#B)$. "Product Principle".

Less formal Statement: Suppose set S can be enumerated by making k choices where there are n_i possibilities for the i^{th} choice made, independent of the other choices themselves. Then $\#S = n_1 n_2 \cdots n_k$.

Ex: Suppose an ice-cream shop has 31 flavours of ice cream, 7 dry toppings, and 10 syrups. How many 3-scoop ice creams can be made using the flavours, one dry topping and one syrup?

Sol: Every 3-scoop ice cream is constructed by the following:

① Choose flavour of first scoop. (31 options)
② choose flavour of 2nd scoop. (31 options)
③ choose flavour of 3rd scoop. (31 options)
④ choose a dry topping. (7 options)
⑤ choose a syrup. (10 options)

The sequence of choices made above uniquely determines the ice cream cone.

∴ by the product principle, there are $31 \cdot 31 \cdot 31 \cdot 7 \cdot 10$ possibilities!

HW: How many possible ice creams w/ 3 scoops can be made at the UP cold stone?

NB: More formally, what I showed via my "sequence of choices" argument is: The possible ice creams are in "one-to-one correspondence" with elements of the product

$$S \times S \times S \times D \times Y \quad \text{where}$$

$S = \{\text{ice cream flavours}\}$, $D = \{\text{dry toppings}\}$, $Y = \{\text{syrups}\}$.

Ex: Suppose we have 7 dice with 20 sides (d20) and 53 dice with 6 sides (d6). How many dice do we have?

Sol: 7 d20 and 53 d6 makes $7+53 = 60$ dice... ☒

Prop: If A, B are sets and $[A \cap B = \emptyset]$ ("A and B are disjoint"), then

$$\#(A \cup B) = \#A + \#B.$$

"Addition Principle".

Ex: How many ice creams can be made at the ice cream shop from earlier w/ 1, 2, or 3 scoops, along w/ 1 dry topping and 1 syrup?

Sol: Let $A_i = \{x : x \text{ is a } i\text{-scoop ice cream}\}$ w/ $i = 1, 2, 3$.
We're asked to count $A_1 \cup [A_2 \cup A_3]$. Note that pairwise $A_i \cap A_j = \emptyset$ for $1 \le i < j \le 3$ (i.e. A_1, A_2, A_3 are pairwise disjoint). Hence $\#(A_1 \cup A_2 \cup A_3) = (\#A_1) + (\#A_2) + (\#A_3)$.

[Exercise: Count A_1, A_2, A_3 separately (use the product principle).]

$\rightsquigarrow \#A_i = 31^i \cdot 7 \cdot 10$. Hence there are

$$31 \cdot 7 \cdot 10 + 31^2 \cdot 7 \cdot 10 + 31^3 \cdot 7 \cdot 10$$

total such ice creams.

Defn: Sets [A and B] are disjoint when $A \cap B = \emptyset$.
The sets in [collection $\mathcal{F}$ of sets] are pairwise disjoint when for all $A, B \in \mathcal{F}$, either $A = B$ or A is disjoint from B.

Prop: If there is a rule of assignment for which every element of set A is assigned one and only one element of set B, and this assignment covers all of B, then $\#A = \#B$.

"Correspondence Principle".

(you don't need to know these words (yet...).)

More Rigorously: If there is a bijection $f : A \to B$, then $\#A = \#B$.

These three Enumeration Principles:

Addition Principle, Product Principle, Correspondence Principle

Are the core principles for enumeration...

Prop: Let S be an n-element set. Then

$$\#\mathbb{P}(S) = 2^n.$$

Pf: Let S be an n-element set. Thus we may list S (in roster notation) by

$S = \{x_1, x_2, \cdots, x_n\}$. Thus, by the correspondence principle, $\#S = \#[n] = n$; the correspondence is $x_i \longleftrightarrow i$.

We use this correspondence to build another correspondence

$\mathbb{P}(S) \longleftrightarrow \mathbb{P}([n])$ via $T \subseteq S \longleftrightarrow \{i \in [n] : x_i \in T\}$.

Hence, we need only show $\#\mathbb{P}([n]) = 2^n$ for all n by the Correspondence principle. We do so by induction on n.

Base Case: When $n = 0$, $[n] = [0] = \emptyset$, so

$\mathbb{P}([n]) = \mathbb{P}(\emptyset) = \{\emptyset\}$, so $\#\mathbb{P}(\emptyset) = 1 = 2^0 = 2^n$.

Thus $\#\mathbb{P}([n]) = 2^n$ in this base case.

Inductive Step: Suppose the result holds for some $n \geq 0$.

I.e. $\#\mathbb{P}([n]) = 2^n$. (WTS: $\#\mathbb{P}([n+1]) = 2^{n+1}$).

Let $T \subseteq [n+1]$ (i.e. let $T \in \mathbb{P}([n+1])$). Either $n+1 \in T$ or $n+1 \notin T$. We let

$A = \{T \subseteq [n+1] : n+1 \notin T\}$ and $B = \{T \subseteq [n+1] : n+1 \in T\}$.

Note $\mathcal{P}([n+1]) = A \cup B$ and $A \cap B = \emptyset$.

Thus $\#\mathcal{P}[n+1] = (\#A) + (\#B)$ by the Addition Principle. Now $A = \mathcal{P}[n]$, whereas $B = \{T \cup \{n+1\} : T \subseteq [n]\}$, so B is in one-to-one correspondence with $\mathcal{P}[n]$ (correspondence is $T \leftrightarrow T \cup \{n+1\}$). Hence $\#A = 2^n$ by induction, and $\#B = \#A = 2^n$ by the correspondence principle. Hence

$$\#\mathcal{P}[n+1] = 2^n + 2^n = 2(2^n) = 2^{n+1}.$$

Hence the original statement holds. ☒

↳ P.S. I was rushing by this point... we'll review this next time :)